



(19)
Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) DE 103 19 778 A1 2004.07.15

(12)

Offenlegungsschrift

(21) Aktenzeichen: 103 19 778.8

(51) Int Cl.: G06F 3/08

(22) Anmeldetag: 30.04.2003

(43) Offenlegungstag: 15.07.2004

(66) Innere Priorität:
102 61 722.8 30.12.2002

(74) Verleiher:
Castell, K., Dipl.-Ing. Univ. Dr.-Ing.; Reuther, M.,
Dipl.-Phys., Pat.-Anw., 52349 Düren

(71) Anmelder:
DATABAY AG, 52068 Aachen, DE

(72) Erfinder:
Schenk, Ralf, 52064 Aachen, DE

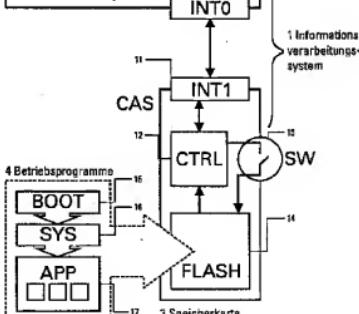
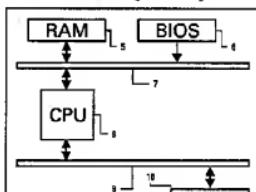
Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: Tragbare Speicherkarte mit einer Schnittstelle, System aus Datenverarbeitungsgerät und entsprechender Speicherkarte sowie Verfahren zum Betrieb eines derartigen Systems

(57) Zusammenfassung: Es wird eine Anordnung vorgeschlagen, die es auch Laien ermöglicht, ein Datenverarbeitungsgerät für spezielle Aufgabenbereiche betriebsicher konfiguriert zu booten.

2 Informationseverarbeitungsvorrichtung



Beschreibung

[0001] Die Erfindung betrifft eine tragbare Speicherkarte mit einer Schnittstelle, ein System aus Datenverarbeitungsgerät und entsprechender Speicherkarte sowie ein Verfahren zum Betrieb eines derartigen Systems.

[0002] An sich sind tragbare Speicherkarten, die mit einer Schnittstelle an ein Datenverarbeitungsgerät angeschlossen werden können und über einen eigenen Controller und Speicher verfügen, schon bekannt. Ein Beispiel hierfür offenbart die DE 197 37 369 A1 in seiner allgemeinsten Form. Eine derartige Speicherkarte kann insbesondere über eine bereits an einem Rechner vorhandene Schnittstelle mit dem entsprechenden Datenverarbeitungsgerät verbunden werden. Hierzu bieten sich nach der DE 19737 369 A1 insbesondere serielle Schnittstellen, und zwar sowohl synchrone als auch asynchrone serielle Schnittstellen oder ähnliches, an. Derartige transportable Speicherkarten bzw. Speichereinrichtungen sind insbesondere auch aus der EP 0 844 554 A2, der GB 2-101-858 A und der EP 0 431 723 A2 aus dem Gebiet der Spiele-Konsolen bekannt, wobei diese Druckschriften sich unter anderem auch mit der Bootfähigkeit der mit derartigen Speicherkarten versehbaren Datenverarbeitungsgeräten beschäftigen, wobei es ankommt, zumindest zwischenzeitlich während der Bootsequenz des Datenverarbeitungsgeräts auf Daten, die in der tragbaren Speicherkarte gespeichert sind, zurückzugreifen, wie auch die DE 199 35 886 A1 offenbart.

[0003] Insbesondere die DE 196 39 687 A1 offenbart eine transportable Speicherkarte, dort als mobiles Speichermedium benannt, welche über eine Extern-Schnittstelle mit einem Datenverarbeitungsgerät bzw. einem Rechnergerät verbunden werden kann und welche einen bootfähigen Sektor, nachfolgend Bootimage genannt, umfasst. Um es einem Nutzer zu ermöglichen, ein Datenverarbeitungsgerät mit den persönlichen Nutzeinstellungen zu konfigurieren und dann personalisiert nutzen zu können, ist auf der transportablen Speicherkarte noch ein Speicher für benutzerspezifische Daten, Dateien und Programme vorgesehen, wobei alle Daten des Nutzers in diesem Speicherbereich abgelegt werden sollen, so dass das Datenverarbeitungsgerät nach einem erneuten Booten ohne die entsprechende Speicherkarte keine Daten desjenigen Nutzers, der seine Speicherkarte wieder entnommen hat, mehr findet. Mit einem solchen System ist es einem Nutzer möglich, auf zum Beispiel Reisen nur die entsprechende Speicherkarte mitzunehmen, vor Ort zum Beispiel ein entsprechendes Notebook oder ein sonstiges Datenverarbeitungsgerät auszuleihen und dann mit seiner Speicherkarte das geliehene Datenverarbeitungsgerät gänzlich in einen vom Nutzer gewünschten Gerätzzustand zu bringen, so dass er in gewohnter Weise arbeiten kann, ohne dass er sein eigenes, an ihn angepasstes Notebook dazu mitführen muss. Wird ein

derartiges Datenverarbeitungsgerät dann ohne diese Speicherkarte gebootet, so wird es wieder in seinen ursprünglichen Betriebszustand betrieben. Um zu gewährleisten, dass bei eingesteckter Speicherkarte auch das Bootimage der eingesteckten Speicherkarte genutzt wird, ist in dem entsprechenden Rechner ein Umschalter vorgesehen, welcher durch das Einstecken der Speicherkarte betätigt wird und welcher zwischen einem internen Bootspeicher des Datenverarbeitungsgeräts und dem Bootimage der tragbaren Speicherkarte umschaltet.

[0004] Im Übrigen ist es jedoch bei Datenverarbeitungsgeräten auch bekannt, verschiedene Speichermedien eines Datenverarbeitungsgeräts in einer definierbaren Weise nach Bootimages bzw. Bootspeichern abzusuchen und dann den als erstes gefundenen Bootbereich zum Booten zu verwenden.

[0005] Alle diese Anordnungen ändern jedoch die entsprechenden Datenverarbeitungsgeräte in ihrer Konfiguration nicht. So bleibt eine Spiele-Konsole eine Spiele-Konsole, auch wenn teilweise aus einer externen bzw. tragbaren Speicherkarte gebootet wird. Ebenso bleibt ein Personal-Computer bzw. ein Notebook nach der DE 196 39 687 A1 ein Personal-Computer bzw. ein Notebook. Andererseits besteht regelmäßig das Problem, Datenverarbeitungsgeräte für spezielle Aufgaben, beispielsweise als Server für Firewalls, VPN (virtual-private-network), WLAN-gateways bzw. Access-Points, Printserver, certification authority, terminal dient, file-server, communication-server, Notfallsysteme oder für ähnliche Aufgaben, auszustatten. Hierzu werden häufig auch kleinere bzw. ältere Rechner eingesetzt. Eine derartige Umgestaltung eines Rechners ist jedoch in der Regel verhältnismäßig komplex und nur von erfahrenen bzw. speziell ausgebildeten Personen durchführbar. Insofern gestaltet sich eine entsprechende Installation als entsprechend zeit- und kostenintensiv, insbesondere wenn mehrere Systeme dementsprechend aus- bzw. umgestaltet werden sollen. Darüber hinaus stehen derartige Fachkräfte häufig nicht ständig zur Verfügung, was insbesondere im Falle von Stromausfällen oder Computerabstürzen dazu führt, dass die entsprechenden Anordnungen nicht unmittelbar wieder zur Verfügung stehen können.

[0006] Es ist Aufgabe vorliegender Erfindung, es auch ungeschulten Nutzern zu ermöglichen, Datenverarbeitungsgeräte zu speziellen Geräten aus- bzw. umzugestalten.

[0007] Als Lösung schlägt die Erfindung eine tragbare Speicherkarte mit einer Schnittstelle, einem Controller und einem Speicher vor, die sich dadurch auszeichnet, dass in dem Speicher zumindest ein Bootimage, ein Betriebssystem und ein Anwendungsprogramm vorgesehen ist.

[0008] Eine derartige Speicherkarte hat den Vorteil, dass durch das Bootimage sowie durch das Betriebssystem ein Standard-Datenverarbeitungsgerät zur Gänze spezialisiert werden kann, so dass es dann für

genau ihm zugewiesene Aufgabe konfiguriert ist. Darüber hinaus ist die Verwendung einer derartigen Speicherplatte über mechanische Festspeicher als Bootsystem und Träger des Betriebssystems von Vorteil, da derartige Speicherplatten einen mechanischen Verschleiß nicht unterliegen und sich deshalb besonders für einen dauerhaften Einsatz, insbesondere auch unter widrigen Bedingungen, eignen. Darüber hinaus können die notwendigen Tätigkeiten von nahezu jeder Person durchgeführt werden, da lediglich die Speicherplatte eingesteckt und ein Bootvorgang initialisiert werden braucht, wobei ein derartiger Bootvorgang ohne Weiteres durch ein Aus- und Einschalten bzw. durch ein Betätigen des am Datenverarbeitungsgerät befindlichen Reset-Knopfes eingeleitet werden kann. Auf diese Weise kann insbesondere bei einem Betriebsausfall das entsprechende System auch von einem Laien neu gestartet werden, wobei insbesondere auf mechanische Festspeicher, wie Laufwerke oder Disketten, die sehr störfähig sind, für die Systemeinrichtung nicht zurückgegriffen werden braucht. Dieser Vorteil zeigt sich insbesondere bei spezialisierten Datenverarbeitungsgeräten, die normalerweise nicht zugänglich sein brauchen, wie bei File-Servers, Firewalls, Kommunikations-Servern und ähnlichen Anordnungen, da diese normalerweise in Nebenräumen abgestellt werden und möglicherweise über Jahre durchlaufen, so dass sie mit der Zeit Staub, Schmutz bzw. elektrostatische Anlagerungen ansammeln. Während derartige Anlegerungen häufig im laufenden Betrieb unkritisch sind, können sie insbesondere eine Neustart des Systems vereiteln, indem die lediglich zum Booten gebrauchten Bereiche mechanischer Speichermedien mit der Zeit unbrauchbar werden.

[0009] Vorzugsweise weist die Speicherplatte einen Schreibschutz auf. Ein derartiger Schreibschutz sollte insbesondere der Gestalt wirken, dass eine Veränderung des Bootimages, des Betriebssystems und nach Möglichkeit auch des Anwendungsprogramms ausgeschlossen werden kann. Auf diese Weise können unbeabsichtigte, aber auch mutwillige Veränderungen in der Gesamtkonfiguration vermieden werden, wodurch die Betriebssicherheit erheblich erhöht werden kann. Insbesondere eignet sich eine derartige Speicherplatte dann auch für Anwendungen mit hohen Sicherheitsanforderungen, beispielsweise für Firewalls.

[0010] Je nach konkreten Sicherheitsanforderungen kann es jedoch auch schon ausreichen, die Speicherplatte nach dem Laden des Anwendungsprogramms zu entfernen, so dass Manipulationen an der Speicherplatte ausgeschlossen werden. Weitergehende Manipulationen können durch geeignete Konfiguration des Datenverarbeitungsgeräts mittels des Bootimages und des Betriebssystems ausgeschlossen werden, indem beispielsweise eine Tastatur überhaupt nicht angesprochen wird.

[0011] Insbesondere, wenn die Speicherplatte entferntbar ist, ist es vorteilhaft, wenn das Ende des La-

dens des Anwendungsprogramms über eine Anzeige dem Nutzer dargestellt wird, so dass dann die Speicherplatte betriebssicher entfernt werden kann. Diese Anzeige kann einerseits über das Datenverarbeitungsgerät erfolgen. Andererseits ist es auch denkbar, dass diese Anzeige an der Speicherplatte, beispielsweise in Form einer Leuchte, vorgesehen ist. [0012] Insbesondere wenn die tragbare Speicherplatte individuell konfiguriert bzw. individuell eingerichtet werden soll, kann ein überbrückbarer Schreibschutz vorteilhaft sein. Dieser Schreibschutz kann einerseits an sich elektronisch von einem Datenverarbeitungsgerät aus ansteuerbar sein oder andererseits mit einem an der tragbaren Speicherplatte vorgesehenen Schreibschutzschalter, der mit einem mechanischen oder elektronischen Schlüssel wechselt, überbrückt werden. Hierbei ist die Gesamtanordnung vorzugsweise derart ausgelegt, dass das Betriebssystem und/oder das Anwendungsprogramm geladen, manipuliert oder konfiguriert werden können, wenn der Schreibschutz geöffnet ist.

[0013] Hierbei kann die Speicherplatte einerseits in Verbindung mit dem Schreibschutz derart ausgestaltet sein, dass Manipulationen des Speichers zumindest im Bootimage bzw. Betriebssystembereich oder dem Bereich des Anwendungsprogramms nur möglich sind, wenn das Datenverarbeitungsgerät auf andere Weise als über das Bootimage der tragbaren Speicherplatte gebootet wurde, da in der Regel ein über die tragbare Speicherplatte als spezielles Gerät konfiguriertes Datenverarbeitungsgerät für derartige Installationstätigkeiten ohnehin nicht ausgelegt sein soll. Insbesondere kann somit die tragbare Speicherplatte separat in geeigneter Weise bereit gestellt bzw. konfiguriert werden, ohne dieses vor Ort und insbesondere mit den möglicherweise eingeschränkten Möglichkeiten des über die tragbare Speicherplatte zu spezialisierenden Datenverarbeitungsgerätes durchführbar ist. Andererseits kann für eine derartige Manipulation bzw. Konfiguration auch dieses Datenverarbeitungsgerät genutzt werden, insbesondere wenn dieses auf andere Weise gebootet wird.

[0014] Als mechanische bzw. elektronische Schlüssel können alle Schlüsselelemente, die einen Schreibschutz für Speicher gewährleisten, zur Anwendung kommen. Insbesondere können auch – je nach gewünschter Sicherheitsstufe – einfache Schalter genutzt werden.

[0015] Wie bereits vorstehend angedeutet, kann es vorteilhaft sein, die in dem Speicher der tragbaren Speicherplatte vorgesehenen Anweisungen in geeigneter Weise zu konfigurieren. Dementsprechend ist es vorteilhaft, wenn die Speicherplatte in ihrem Speicher einen Konfigurationspeicher zum Abspeichern wenigstens einer für das Anwendungsprogramm vorgesehenen Konfiguration aufweist. Hierbei muss dieser Konfigurationspeicher nicht zwingend sämtlich zur Konfiguration notwendigen Daten umfassen, so dass einzelne Daten, wie beispielsweise der Name des jeweiligen Nutzers, auch separat angefragt wer-

den können. Vorzugsweise ist der Konfigurationsspeicher ebenfalls über den Schreibschutz gesichert. [0016] Vorzugsweise ist der gesamte Speicher der Speicherkarte derart schreibgeschützt, dass unbeabsichtigt keine Daten auf der Speicherkarte verändert werden können. Hierdurch werden Manipulationen zur Gänze ausgeschlossen bzw. können mit einer gewünschten Sicherheitsstufe verhindert werden. Der Schreibschutz kann hierbei permanent bzw. ein- und ausschaltbar ausgebildet sein, wie bereits vorstehend beschrieben.

[0017] Vorzugsweise umfasst der Speicher der tragbaren Speicherkarte einen Flash-Speicher, also eine nicht flüchtigen Speicher, so dass das Bootimage, das Betriebssystem sowie das Anwendungsprogramm auch über längere Zeit ohne weitere Maßnahmen möglichst betriebssicher zur Verfügung stehen. Hierzu bieten sich insbesondere EEPROM (electrical erasable EPROM) an. Denkbar sind jedoch auch andere Permanent-Speicher bzw. Batterie- bzw. sonst wie gepufferte Speicher.

[0018] Die Erfindung setzt sich auf besonders einfache Weise um, wenn als Schnittstelle eine serielle Schnittstelle zur Anwendung kommt. Eine derartige Schnittstelle ist in nahezu allen Datenverarbeitungsgeräten vorhanden und in der Regel auch ohne weiteres zugänglich. Voraussetzung ist, dass über diese Schnittstelle insbesondere ein Booten möglich ist, es sich hierbei also um eine bootfähige Schnittstelle handelt. Hierzu eignet sich insbesondere eine USB-(universal-serial-bus)-Schnittstelle, die nahezu in jedem Computer vorhanden und in der Regel besonders einfach zugänglich und bedienbar ist. Insbesondere mit einer derartigen Schnittstelle ausgestattete, bootfähige Memory-Cards können demnach in erfundungsgemäßer Weise ausgestaltet werden. Derartige Memory-Cards sind mittlerweile verhältnismäßig kostengünstig und sind darüber hinaus robust und verhältnismäßig betriebssicher.

[0019] Eine erfundungsgemäße tragbare Speicherkarte ermöglicht es, zunächst die Speicherkarte über die Schnittstelle mit dem Datenverarbeitungsgerät zu verbinden, anschließend das Datenverarbeitungsgerät über das Bootimage der Speicherkarte zu booten, das Betriebssystem zu aktivieren und das Anwendungsprogramm zu starten. Nach dem Start des Anwendungsprogramms kann – je nach konkreter Umsetzung der Erfindung – die Speicherkarte entnommen werden.

[0020] Insofern benötigt ein Datenverarbeitungsgerät nicht zwingend Festspeicher bzw. Laufwerke, insbesondere für Wechselspeichemedien. Dieses spart Kosten und belässt die entsprechenden Datenverarbeitungsgeräte störungsunanfälliger. Darüber hinaus können kleinere, für den jeweiligen Einsatzzweck optimierte Datenverarbeitungsgeräte verwendet werden. Auch können bereits bestehende Datenverarbeitungsgeräte schnell und unkompliziert für entsprechende Spezialaufgaben eingerichtet werden. Insbesondere ist es nicht notwendig, Betriebssysteme und

Anwendungen manuell auf den jeweiligen Geräten zu installieren, da die notwendigen Anwendungsprogramme und das Betriebssystem ebenfalls auf der Speicherkarte untergebracht sind. Dies kann insbesondere in Netzwerkumgebungen die Wartung und Aktualisierung von Software vereinfachen.

[0021] Insbesondere wenn die Speicherkarte nach dem Hochfahren des Datenverarbeitungsgeräts entfernt ist, sind die jeweiligen Programme vor einem Zugriff durch das System selbst geschützt. Fehler, die durch die Benutzung entstehen, oder Manipulationen aufgrund von feindlichen oder versehentlichen Eindringens in das System können sich nicht auf den abgenommenen Speicher und somit auf das Bootimage, das gespeicherte Betriebssystem und das gespeicherte Anwendungsprogramm auswirken. Insbesondere wenn auf sonstige Festspeicher in dem entsprechenden Datenverarbeitungsgerät verzichtet wird, kann durch einfaches Rebooten, nachdem die Speicherkarte wieder eingestellt ist, „Jungfräulich“ gestartet werden, so dass alle vorherigen Manipulationen unwirksam sind, da diese nirgendwo permanent gespeichert werden können.

[0022] Ist ein aufhebbarer Schreibschutz vorgesehen, so kann in einer sicheren Umgebung das Betriebssystem bzw. das Anwendungsprogramm, aber auch der Bootbereich, aktualisiert werden.

[0023] Die Erfindung ermöglicht es darüber hinaus, voll installierte Arbeitsplatz-Computer oder Server-Computer temporär oder dauerhaft anders zu nutzen ohne die bisherige Installation anzutasten, da über das Bootimage und das Betriebssystem der Speicherkarte eine eigene Umgebung geschaffen werden kann. Sofern von der Speicherkarte die Betriebssystem- und Anwendungsumgebung gebietet wird, ermöglicht das Computersystem somit eine völlig andersartige Nutzung auf Basis der jeweiligen Betriebsprogramme, und zwar ohne von einem alten, womöglich kompromittierten, Betriebssystem beeinflusst zu werden. Wird nach dem Entfernen der Speicherkarte des Rechners neu gestartet, so steht die gewohnte, alte Anwendungsumgebung zur Verfügung.

[0024] Als Schnittstelle kann insbesondere auch eine Firewire-Schnittstelle zur Anwendung kommen, die einen ebenfalls bootfähigen Zugang zu einer Datenverarbeitungsanlage ermöglicht.

[0025] Darüber können Mittel für eine Benutzerauthentifizierung vorgesehen sein, wobei diese einerseits separat, beispielsweise über das Datenverarbeitungsgerät, oder andererseits auch direkt auf der Speicherkarte wirksam sein können. Insofern kann die Schnittstelle vorteilhafter Weise auch ein Protokoll zur Benutzerauthentifizierung umfassen, mit welchem letztere über das Datenverarbeitungsgerät durchgeführt werden kann. Vorzugsweise bleibt das Betriebssystem und/oder das Anwendungsprogramm nur aktiv bzw. startet das Betriebssystem und/oder das Anwendungsprogramm ausschließlich, wenn eine entsprechende Benutzerauthentifizierung erfolgt ist.

[0026] Vorzugsweise befindet sich auf der erfundungsgemäßen Speicherplatte wenigstens ein weiteres Anwendungsprogramm, das unter einem anderen Betriebssystem als dem auf der Speicherplatte zu startendem Betriebssystem ausgeführt werden kann bzw. muss. Dieses ist dann derart ausgestaltet, dass es einen Betrieb der Speicherplatte, insbesondere eines auf der Speicherplatte befindlichen Controllers, zum Abspeichern von Daten, Programmen bzw. Konfigurationen, ermöglicht. Auf diese Weise können die entsprechenden Daten in einer anderen, von einer durch Booten von der Speicherplatte geschaffenen Umgebung abweichenden Umgebung auf die Speicherplatte gebracht werden. Auf diese Weise kann ohne Weiteres sichergestellt werden, dass die entsprechenden Daten nicht unbeabsichtigt manipuliert werden können.

[0027] Weitere Vorteile, Ziele und Eigenschaften vorliegender Erfindung werden anhand der Beschreibung anliegender Zeichnung erläutert, in welcher beispielhaft Systeme sowie die Durchführung des erfundungsgemäßen Verfahrens dargestellt sind. In der Zeichnung zeigen:

[0028] Fig. 1 einen schematischen Aufbau eines erfundungsgemäßen Systems;

[0029] Fig. 2 die Umsetzung der Erfindung bei einem Desktop-PC;

[0030] Fig. 3 die Umsetzung der Erfindung bei einem Tower-PC;

[0031] Fig. 4 die Umsetzung der Erfindung bei einem Rackserver; und

[0032] Fig. 5 den Verfahrensablauf anhand des in Fig. 2 erläuterten Ausführungsbeispiels.

[0033] Das in Fig. 1 exemplarisch und schematisch dargestellte Informationsverarbeitungssystem 1 umfasst einerseits eine Informationsverarbeitungsvorrichtung bzw. ein Datenverarbeitungsgerät 2 und andererseits eine Speicherplatte 3, welche Betriebssysteme 4 enthält. Wie an sich bei Computern üblich, weist die Informationsverarbeitungsvorrichtung 2 dieses Ausführungsbeispiels flüchtige Speicher 5 (RAM) und Nur-Lese-Speicher 6 (BIOS) auf, die über einen Systembus 7 mit einem Zentralprozessor 8 verbunden sind. Darüber hinaus umfasst die Informationsverarbeitungsvorrichtung 2 einen Eingabe-Ausgabe-Bus 9, der mit einer seriellen Schnittstelle 10 der Informationsverarbeitungsvorrichtung 2 verbunden ist. Es versteht sich, dass die Busse 7 und 9 auch mit weiteren Komponenten Wechselwirken können.

[0034] Die Speicherplatte 3 ist ebenfalls mit einer seriellen Schnittstelle, der seriellen Schnittstelle 11, ausgerüstet. Sie verfügt über einen Controller 12, der einerseits Daten aus einem nicht flüchtigen Speicher 14 Daten lesen und der Informationsverarbeitungsvorrichtung 2 zur Verfügung stellen kann. Über einen manuellen Schalter 13 kann der Controller 12 in die Lage versetzt werden, Daten auch in den Speicher 14 zu schreiben. Bei vorliegendem Ausführungsbeispiel enthält der Speicher 14 ein Bootimage 15, ein Betriebssystem 16 und Anwendungsprogramme 17.

Vorzugsweise simuliert der Controller 12 gegenüber der Informationsverarbeitungsvorrichtung 2 ein Festplatten. Für das Zielsystem 2 verhält sich dann die Speicherplatte 3 wie ein Festplatten. Anders als bei anderen bootfähigen Speicherplatten braucht dann das Zielsystem 2 lediglich den Bootvorgang für eine über eine serielle Standardschnittstelle angeschlossene Festplatte zu unterstützen. Das trifft auf die größere Zahl der derzeit am Markt befindlichen PC-Hauptplatten zu als die direkte Unterstützung einer bootfähigen Speicherplatte für serielle Standardschnittstellen. [0035] Vorliegend kann das Bootimage 15 ein Datapaket sein, an dessen Anfang ein sofort vom Prozessor 8 des Zielsystems 2 ausführbarer Maschinencode, ein sogenannter Bootloader, steht. Dieser wird vom BIOS eines PC bzw. von dem Nur-Lese-Speicher 6 der Informationsverarbeitungsvorrichtung 2 erkannt und auf einem bootbaren Datenträger erwartet. Das BIOS startet nach dem Erkennen des des Bootloaders umfassenden Bootsektors den Bootloader. Der Bootloader übernimmt und bestimmt das weitere Vorgehen. Beispielsweise kann der Bootloader vorliegend auch einen Betriebssystemkern laden, der bereits rudimentäre Funktionen eines Serverbetriebssystems zur Verfügung stellt. Danach kann der weitere Ladevorgang an das Betriebssystem übergeben werden.

[0036] Das Betriebssystem ist in der Regel eine umfassende Sammlung von Programmen und Programmmodulen, die in erster Linie dazu dient, Anwendungsprogrammen einheitliche Schnittstellen und ein Abstraktionsmodell der Hardwarekomponenten zur Verfügung zu stellen. Das Betriebssystem kommuniziert vorzugsweise direkt mit der Hardware. Beispielsweise kann es sich vorliegend um ein auf Betriebssicherheit optimiertes Betriebssystem 16 handeln, das eine große Anzahl an Geräten und Standardhardware unterstützt und sich auch Serverbetriebssystem mit umfassender Unterstützung aktueller Netzwerktechnologien eignet. Es bietet die Basis für Anwendungsprogramme, die auf den jeweiligen Einsatz hin entwickelt sind. Vorzugsweise findet ein OpenSource-Betriebssystem in vorliegendem Zusammenhang Anwendung, dessen Quellen frei erhältlich und einsehbar sind. Dieses bietet besondere Vorteile in Hinblick auf Wartung, Fehlerbehebung und Zukunftssicherheit.

[0037] Die Anwendungsprogramme 17 führen das Zielsystem 2 über die spezielle Zusammenstellung des Betriebssystems hinaus einem bestimmten Zweck für den jeweiligen konkreten Einsatz, beispielsweise in einem speziellen Unternehmens- und Infrastrukturfeld zu. Sie werden vorzugsweise automatisch gestartet und laden ihre Konfiguration, so weit sie notwendig ist, vorzugsweise von der Speicherplatte 3. Sie erfordern vorzugsweise keine Interaktion mit einem Nutzer. Somit kann beispielsweise ein kompletter Server mit individueller Konfiguration ohne Eingriff eines Nutzers, d.h. ohne Tastatur- oder sonstige Eingaben hochgefahren werden.

[0038] Bei vorliegendem Ausführungsbeispiel kann das Bootimage 15 bzw. das Betriebssystem 16 derart ausgestaltet sein, dass diese ein Ändern des Speichers 14 nicht ermöglichen, wenn von der Speicher-karte 3 gebootet werden ist. Auf diese Weise ist ausgeschlossen, dass die Speicher-karte 3 manipuliert werden kann, wenn die Informationsverarbeitungsvorrichtung 2 in ihrem speziellen, durch die Speicher-karte 3 definierten Modus betrieben wird. Ansonsten kann jedoch bei entsprechend eingestelltem Schalter 13 in einer normalen PC-Umgebung eine Manipulation vorgenommen werden. Die Sicherheit lässt sich weiter erhöhen, indem statt des Schalters 13 ein über einen Schlüssel zu betätigender Schalter verwendet wird. Ebenso kann kumulativ bzw. alternativ ein elektronischer Schlüssel vorgesehen sein, der erst Manipulationen verhindert bzw. wahlweise ermöglicht. Auf diese Weise kann sichergestellt werden, dass derartige Manipulationen nur in einer gesicherten Umgebung erfolgen.

[0039] Durch den Schreibschutz können Anwendungen an anderer Stelle bzw. in anderer Umgebung beispielsweise von einem versierten Anwender vor konfiguriert werden. Vorzugsweise befinden sich auf der erfindungsgemäßen Speicher-karte weitere Anwendungsprogramme, die unter einem anderen Betriebssystem als dem auf der Speicher-karte zu startendem Betriebssystem ausgeführt werden können. Diese Anwendungen ermöglichen dann beispielsweise die Vorkonfiguration. Die individuellen Einstellungen werden dann auf die Speicher-karte geschrieben und stehen beim nächsten Bootvorgang zur Verfügung.

[0040] Das System nach Fig. 1 bzw. das erfindungsgemäße System kann beispielsweise bei einem Desktop-PC 18, einem Tower-PC 19 bzw. einem Rackserver 20 realisiert werden. Hierzu kann beispielsweise eine der Speicher-karte 3 entsprechende tragbare Speicher-karte 21 in einer serielle Schnittstelle, insbesondere eine USB-Schnittstelle dieser Geräte eingesetzt werden, wie anhand der Fig. 2 bis 4 dargestellt. Vorzugsweise wird die Speicher-karte 21 vor einem Hochfahren des entsprechenden Geräts eingesteckt. Anschließend wird dieses eingeschaltet bzw. hochgefahren, wobei beispielsweise eine Anzeige „BOOTING“ den Nutzer darüber informiert, dass ein Ladevorgang abläuft, der vorzugsweise auch das Starten des Betriebssystems und laden und Starten der Anwendungsprogramme umfasst. Ist dieser Abgeschlossen so kann dieses dem Nutzer beispielsweise durch ein „Ready“ angezeigt werden, so dass dieser die Speicher-karte 21 trennen und anderweitig verwenden bzw. sich verwahren kann. Das Gerät ist dann entsprechend konfiguriert und betriebsbereit.

[0041] Eine konkrete Anwendung kann den Einsatz als „Firewall-Applikation“ betreffen. Die Speicher-karte 3 mit einem Schreibschutz wird hierzu mit einem besonders sicheren Betriebssystem und mit Anwendungsprogrammen zum Schutz eines Netzwerks vor unerwünschtem Eindringen bzw. ungewollten Verbin-

dungen nach außen ausgestattet. Ein Computersystem mit flüchtigem Speicher (RAM) und serieller Standardschnittstelle (z.B. USB) sowie Netzwerkkarte wird mit dieser Speicher-karte versehen und hochgefahren. Danach kann die transportable Speicher-karte entfernt werden und das Computersystem fertig konfiguriert als „Firewall“, als Einrichtung zwischen vertrauten und nicht vertrauenswürdigen Netzwerken, die alle Netzwerkkommunikation kontrolliert ggf. filtert und erlaubt oder verbietet, das Netzwerk schützen. Eine Manipulation der Betriebsprogramme und der Konfiguration ist nicht möglich, weil sich die entsprechenden Komponenten nicht mehr im Zugriff des Computersystems befinden. Im Falle eines Hardwaerausfalls oder unerwarteter Systemfehler kann ein anderes intaktes Computersystem mit derselben Kombination aus Speicher-karte und Betriebsprogrammen hochgefahren werden und das defekte System vollständig ersetzen.

[0042] Ebenso kann die Erfindung zur Bildung einer VPN(virtual-private-network)-Gateways genutzt werden. Ein derartiges Gateway ermöglicht den Betrieb eines Computersystems als Verbindungspunkt mit Sicherheitsfunktion zur Kopplung eines oder mehrerer Netzwerke oder Einzelcomputer mit Netzwerken. Hierbei erfolgt die Kopplung über andere, nicht kontrollierte Netzwerke, wie beispielsweise das Internet, hinweg, so als seien die auf diese Weise verbundene Rechner bzw. Netzwerke ein einziges Netzwerk. Die nicht kontrollierte Verbindung wird häufig als Tunnel bezeichnet. Protokolle, wie beispielsweise IPsec ermöglichen eine stark verschlüsselte Übertragung von Nutzdaten und sichere Authentifizierung der sich verbindenden Parteien. Somit kann der Netzwerkeverkehr, obwohl er über nicht kontrollierte Netze erfolgt, nicht eingesehen und missbraucht werden. Die Anwendung entspricht der Vorgehensweise aus der Firewall-Anwendung. Dazu werden auf der transportablen Speicher-karte 3 Bootimage, gehärtetes Betriebssystem, „Firewall“-Anwendungsprogramme und VPN-Anwendungsprogramme sowie die entsprechende Konfiguration gespeichert.

[0043] Die Erfindung kann auch zur Schaffung sicherer, abgeschlossener Systemumgebungen für sicherheitsrelevante Einsatzwecke herangezogen werden, beispielsweise als Zertifizierungsautorität. Hierzu kann ein Arbeitsplatzcomputer von einer erfindungsgemäßen Speicher-karte mit geschütztem Bootimage, mit gehärtetem Betriebssystem und mit ausschließlich für den Einsatzzweck bestimmten Anwendungsprogrammen hochfahren. Der Arbeitsplatzrechner bietet dann für die Zeit bis zum Neustart ohne diese Speicher-karte eine gesicherte Umgebung um Sicherheitszertifikate und Schlüsselcodes zu erzeugen und zu verwalten, und somit als Certification Authority bzw. als Zertifizierungsautorität zu dienen. An eine solche Einrichtung werden besonders hohe Sicherheitsanforderungen gestellt, weil sie die Schlüssel für Zugriffe auf gesicherte Netzwerkdienste, z.B. VPN-, WLAN-Access- oder E-Mail-Verschlüs-

selung, erstellt und verwaltet. Hier erweist sich vorliegende Erfindung als besonders geeignet, da sie die gesamte Betriebssystem- und Anwendungsumgebung bereitstellt und somit eine kontrollierte und isolierte Einrichtung, nach Bedarf nur für einen bestimmten Zeitraum, schafft.

[0044] Ebenso kann eine Speicherplatte derart ausgestaltet werden, dass dedizierte Dienste, beispielsweise ein Druckserver, verfügbar gemacht werden. Ein Standardcomputer kann dann, entsprechend der vorstehend beschriebenen Vorgehensweisen über die erfundungsgemäße Speicherplatte zu einer spezialisierten Komponente für diese Dienste gewandelt werden. Hierbei ist ein Printserver ein spezialisiertes Netzwerkgerät, an welches Drucker sowie ein Intranet angeschlossen werden. Der Printserver verarbeitet Druckaufträge, die über das Intranet an angeschlossene Drucker gesandt werden, und verarbeitet in der Regel die Druckdaten in geeigneter Weise auf.

[0045] Darüber hinaus ist es möglich, eine erfundungsgemäße Speicherplatte derart mit Bootimage, Betriebssystem und Anwendungsprogrammen auszustatten, dass hierdurch eine Wartungsumgebung erzeugt wird, wenn ein Computer hochgefahren wird. Diese Wartungsumgebung kann genutzt werden, falls ein Computersystem aufgrund eines Programmfehlers oder eines Defektes beispielsweise der Festspeicher oder eines Wechselplattenlaufwerks seinen Dienst versagt, um diesen Fehler oder Defekt zu diagnostizieren oder zu beheben.

[0046] Ebenso kann mit einer erfundungsgemäßen Speicherplatte ein bestehender Standardcomputer temporär oder dauerhaft in einen Terminalcomputer mit spezifischer Anwendungsumgebung und Benutzerkonfiguration gewandelt werden. Die Vorgehensweise entspricht hierbei vorzugsweise der zuvor beschriebenen. Hierbei stelle ein Terminalcomputer ein minimales Betriebssystem bereit, das den Zugriff und die Arbeit im Netzwerk ermöglicht. Insbesondere werden Anwendungssoftware und Daten an anderen Stellen, an einer Mainframe o.ä., gehalten und ausgeführt bzw. bearbeitet. Da die Erfindung vorkonfigurierbar ist, kann eine individuelle Umgebung mit bestimmten Zugriffsrechten an eine erfundungsgemäße Speicherplatte gebunden und einer Person übergeben werden. So wird ohne weiteren Installationsaufwand an jedem Netzwerkarbeitsplatz, der für die Erfindung geeignet ist, ein personalisierten Terminal nach Bedarf verfügbar gemacht.

[0047] Auch kann eine erfundungsgemäße Speicherplatte derart ausgestaltet werden, dass durch sie ein WLAN-Gateway und Access-Point bereitgestellt werden kann. Bei ersterem handelt es sich um definierte Netzwerkknoten, über die drahtlos angebundene Geräte in ein Netzwerk eingebunden werden. Spezielle Regeln für einen Zugriffsschutz und eine Anmeldung sichern das jeweilige interne Netzwerk vor unerwünschten Zugriffen per Funk. Ein Access-Point ist die Netzwerkschnittstelle mit dem Funkempfänger für den drahtlosen Netzwerkverkehr. Sie kann vor-

zugsweise in das WLAN-Gateway integriert werden. Insbesondere ist es auch denkbar, die entsprechend notwendige Antenne, oder auch eine andere Schnittstelle, wie beispielsweise ein IR-Schnittstelle oder ähnliches, direkt in die erfundungsgemäße Speicherplatte zu integrieren.

[0048] In ähnlicher Weise kann ein Fileserver, ein Kommunikationsserver bzw. ein Notfallsystem bereitgestellt werden. Ein Fileserver sichert Daten auf einem leistungsfähigen Speicher mit speziellen Sicherheits- und Wiederherstellungsfunktionen. Er ist besonders gegen Fehler und Hardwareausfälle gesichert sowie auf Datendurchsatz optimiert. Hier bringt das in der erfundungsgemäßen Speicherplatte implementierte Betriebssystem vorzugsweise Dateisysteme mit, die sich besonders für den Einsatz in Fileservern eignen. Ein Kommunikationsserver ist auf besondere Anwendungen hin optimiert, die Kommunikationsdienste, wie Telefax, E-Mail, News, FTP, http u.ä. ermöglichen. Die Stabilität und Sicherheit gegen Systemausfälle ist hierbei von besonderer Wichtigkeit. Gegebenenfalls werden auch bestimmte Filter eingesetzt, die die Auslastung verteilen. Das erfundungsgemäße System lässt auch hier maßgeschneiderte Lösungen zu, die einfach zu implementieren sind. Darüber hinaus kann über eine erfundungsgemäße Speicherplatte ein einfach zu handhabendes Notfallsystem bereitgestellt werden. Ein defektes System oder ein beliebiger Netzwerkcomputer kann mit der erfundungsgemäßen und geeignet ausgestatteten Speicherplatte hochgefahren werden und stellt dann Diagnose- und Reparaturwerkzeuge zur Verfügung, um beispielsweise Daten zu retten, Fehler zu beheben oder Systeme wieder herzustellen.

Bezugszeichenliste

- 1** Informationsverarbeitungssystem
2 Informationsverarbeitungsvorrichtung (Datenspeicherungsgerät)
3 Speicherkarte
4 Betriebssysteme
5 Flüchtiger Speicher
6 Nur-Lese-Speicher
7 Systembus
8 Zentralprozessor
9 Eingabe-Ausgabe-Bus
10 Serielle Schnittstelle
11 Serielle Schnittstelle
12 Controller
13 Manueller Schalter
14 Nicht flüchtiger Speicher
15 Bootimage
16 Betriebssystem
17 Anwendungsprogramme
18 Informationsverarbeitungssystem am Beispiel Desktop-PC
19 Informationsverarbeitungssystem am Beispiel Tower-PC
20 Informationsverarbeitungssystem am Beispiel Rackserver
21 Tragbare Speicherkarte

Patentansprüche

- 1.** Tragbare Speicherkarte, umfassend eine Schnittstelle, einen Controller und einen Speicher, dadurch gekennzeichnet, dass in dem Speicher zumindest ein Bootimage, ein Betriebssystem und ein Anwendungsprogramm vorgesehen ist.
- 2.** Speicherkarte nach Anspruch 1, gekennzeichnet durch einen Schreibschutz.
- 3.** Speicherkarte nach Anspruch 2, gekennzeichnet durch einen, insbesondere mit einem mechanischen oder elektronischen Schlüssel versehenen, Schreibschutzschalter.
- 4.** Speicherkarte nach Anspruch 2 oder 3, gekennzeichnet durch einen elektronischen Schreibschutz.
- 5.** Speicherkarte nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass in dem Speicher ein Konfigurationsspeicher zum Abspeichern wenigstens einer für das Anwendungsprogramm vorgesehenen Konfiguration vorgesehen ist.
- 6.** Speicherkarte nach einer der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass der Speicher zumindest einen Flashspeicher umfasst.
- 7.** Speicherkarte nach Anspruch 6, dadurch gekennzeichnet, dass in dem Flashspeicher das Booti-
- mage, das Betriebssystem und das Anwendungsprogramm vorgesehen ist.
- 8.** Speicherkarte nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass die Schnittstelle eine serielle Schnittstelle, vorzugsweise eine USB-Schnittstelle ist.
- 9.** Speicherkarte nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass die Schnittstelle eine Firewire-Schnittstelle ist.
- 10.** Speicherkarte nach einem der Ansprüche 1 bis 9, gekennzeichnet durch Mittel für eine Benutzeroberflächentwurfserkennung.
- 11.** Speicherkarte nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, dass die Schnittstelle ein Protokoll zur Benutzerauthentisierung umfasst.
- 12.** Speicherkarte nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, dass auf der Speicherkarte wenigstens ein weiteres Anwendungsprogramm vorgesehen ist, das unter einem anderen Betriebssystem als dem auf der Speicherkarte zu startenden Betriebssystem ausgeführt werden kann bzw. muss.
- 13.** System aus Datenverarbeitungsgerät und Speicherkarte nach einem der Ansprüche 1 bis 12, dadurch gekennzeichnet, dass die Speicherkarte mit ihrer Schnittstelle an einer komplementären Rechnerschnittstelle angeordnet ist.
- 14.** System nach Anspruch 13, dadurch gekennzeichnet, dass die Rechnerschnittstelle von außen zugänglich ist.
- 15.** System nach Anspruch 13 oder 14, dadurch gekennzeichnet, dass die Speicherkarte nach dem Laden des Anwendungsprogramms entferbar ist.
- 16.** System nach Anspruch 15, gekennzeichnet durch eine Anzeige an der Speicherkarte, die das Ende des Ladens des Anwendungsprogramms anzeigen, so dass dann die Speicherkarte betriebssicher entfernt werden kann.
- 17.** System nach einem der Ansprüche 13 bis 16, dadurch gekennzeichnet, dass die Schnittstelle zwischen der Speicherkarte und dem Datenverarbeitungsgerät ein Protokoll zur Benutzerauthentisierung und das Datenverarbeitungsgerät Mittel für eine Benutzerauthentisierung umfasst.
- 18.** Verfahren zum Betrieb eines Systems aus Datenverarbeitungsgerät und Speicherkarte nach einem der Ansprüche 13 bis 17, dadurch gekennzeichnet, dass zunächst die Speicherkarte über die Schnittstelle mit dem Datenverarbeitungsgerät ver-

bunden, anschließend das Datenverarbeitungsgerät über das Bootimage der Speicherkarte gebootet, dann das Betriebssystem aktiviert und das Anwendungsprogramm gestartet wird.

19. Verfahren nach Anspruch 18, dadurch gekennzeichnet, dass die Speicherkarte nach dem Start des Anwendungsprogramms entfernt wird.

20. Verfahren nach einem der Ansprüche 18 oder 19, dadurch gekennzeichnet, dass Mittel zur Benutzerauthentifizierung vorgesehen sind und das Betriebssystem und/oder das Anwendungsprogramm nur aktiv bleiben bzw. nur starten, wenn eine Benutzerauthentifizierung erfolgt ist.

Es folgen 3 Blatt Zeichnungen

2 Informationsverarbeitungsvorrichtung

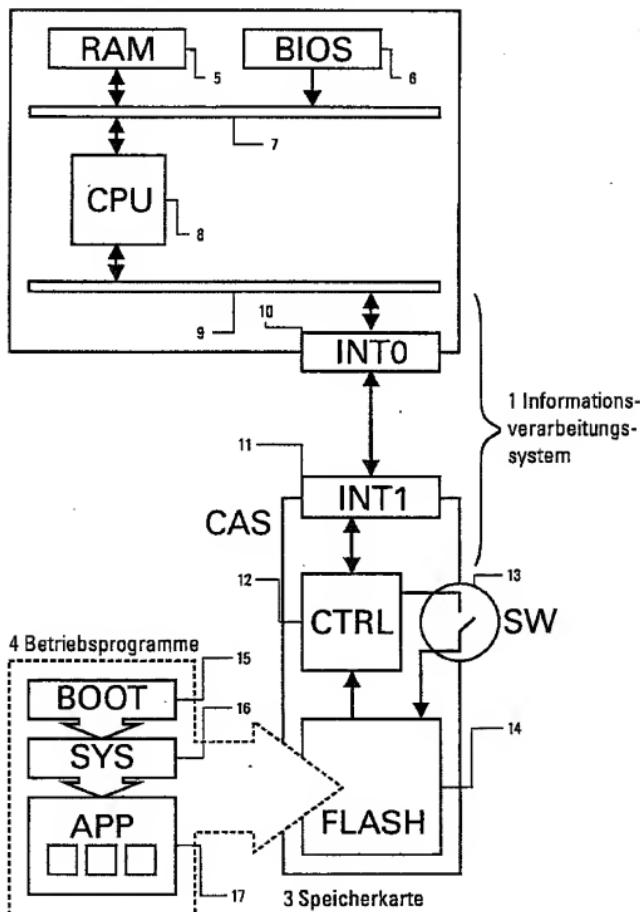
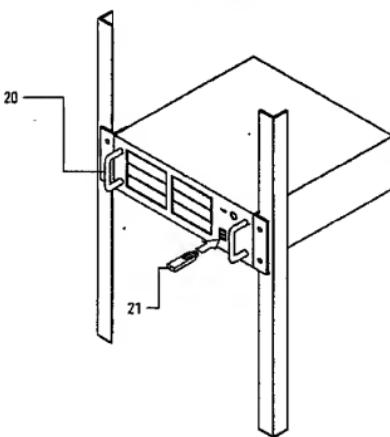
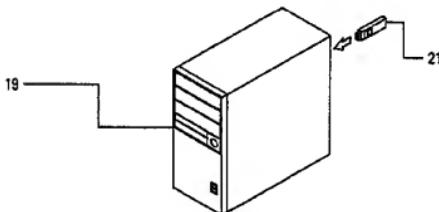
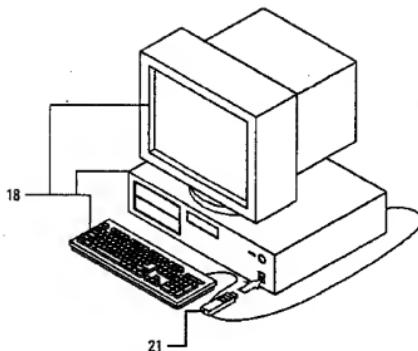


FIG. 1



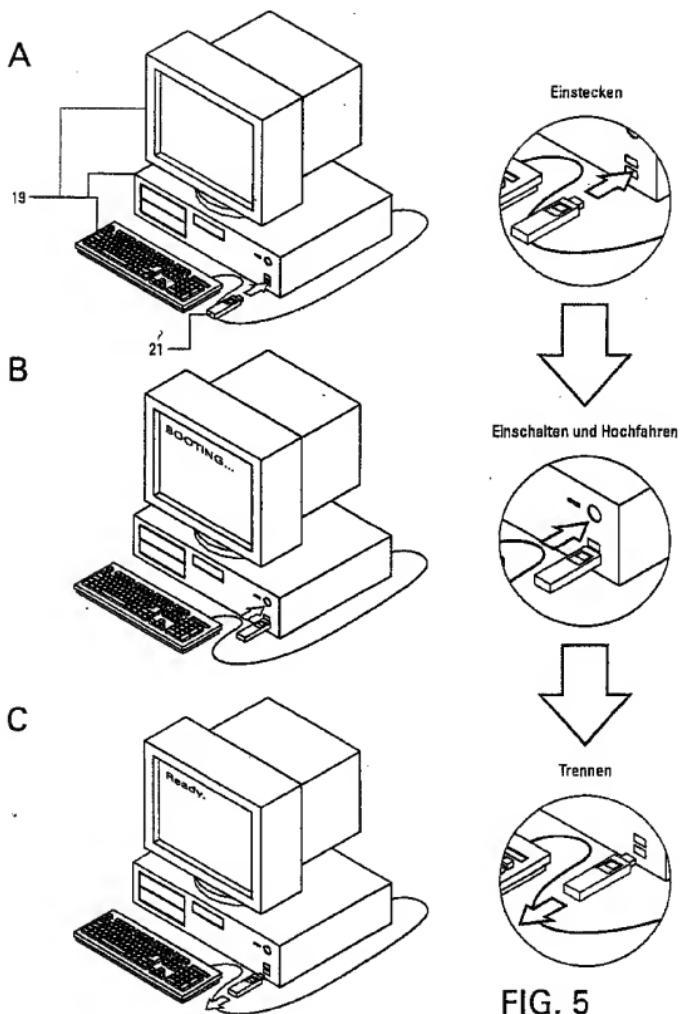


FIG. 5